O FATOR CONFIANÇA

O papel da segurança virtual em manter o ímpeto do negócio

Resumo executivo

Em 2018, os riscos de ciberataques foram mais altos do que nunca. Incidentes chocantes de segurança de dados continuavam a aparecer nas notícias, incluindo o maior ataque de negação de serviço distribuído jamais registrado de 1,7 Tbps.[1] Na União Europeia, o Regulamento Geral sobre Proteção de Dados (GDPR) entrou em vigor em 25 de maio de 2018, impondo novas regras estritas sobre como as informações pessoas identificáveis (PII) são coletadas, processadas e controladas. Além disso, mineradores de criptomoedas se infiltraram nas redes para obter ganhos rápidos.

Entramos em uma era da "pós-confiança", em que as organizações e os indivíduos estão cada vez mais desconfiados em aceitar promessas de segurança por seu valor nominal. Cada vez que os consumidores interagem com uma marca, eles tomam a decisão se confiam o suficiente em uma empresa para compartilhar suas PII. Ciberataques bem-sucedidos quebram a confiança que as empresas trabalharam tão arduamente para estabelecer entre suas marcas e os clientes. As ramificações não são mais de única responsabilidade dos profissionais de segurança; os executivos das diretorias também são responsáveis.

Para oferecer insights sobre os desafios complexos enfrentados pelas organizações enquanto lutam para proteger suas marcas, a Radware produz um Relatório Global de Segurança de Redes e Segurança de Aplicações. Esta oitava versão anual do relatório combina a pesquisa orgânica da Radware, dados de ataques reais e análises de tendências e tecnologias em desenvolvimento com as descobertas de uma pesquisa global no setor.

O relatório destaca o impacto nos negócios e na tecnologia da segurança virtual, incluindo:

- Lições aprendidas de ataques recentes
- Os verdadeiros custos dos ciberataques, tanto quantitativos como qualitativos
- Uma visão geral do cenário de ameaças de rede e de aplicação
- Insights sobre as vulnerabilidades das tecnologias emergentes
- Previsões para 2019

PRINCIPAIS DESCOBERTAS

Equilíbrio entre o custo e o risco calculado

Proteger-se contra ciberataques exige um investimento significativo que recai no lado das despesas operacionais da folha orçamentária. Por natureza, as organizações estão sempre buscando formas de conservar os fundos. Mas quanto é o suficiente ao levar em consideração o risco dos ciberataques penetrarem as defesas e impactarem os negócios?

Considere estes insights reveladores da pesquisa global do setor de 2018-2019 da Radware.

- Em apenas um ano, os custos iniciais atribuíveis aos ciberataques aumentaram em 52% a US$ 1,1 milhão
- As organizações que modelaram os custos gerais dos ciberataques às suas empresas estimaram a quantia em quase o dobro em comparação com as empresas que não modelaram estes custos
- Duas em cada cinco empresas relataram experiências de cliente negativas e perda de reputação logo após um ataque bem-sucedido
- Um total de 93% dos participantes da pesquisa passaram por um ciberataque nos últimos 12 meses; apenas 7% declararam não ter passado por um ataque
- Os ciberataques eram uma ocorrência semanal para um terço das organizações
- O impacto principal dos ciberataques foi a interrupção do serviço, relatada em quase metade dos participantes. Os ataques que resultam em interrupção total ou parcial de serviços cresceram em 15% e prejudicaram a produtividade
- O resgate virtual continuou a ser a motivação principal dos hackers e foi o motivo de 51% dos ataques

[1] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/memcache-ddos-as-a-service/

Vetores de ataque emergentes

Os atacantes empregam técnicas eficientes para causar negação de serviço, como bursts, amplification, criptografia ou botnets da Internet das Coisas (IoT), e visam a camada da aplicação para causar mais prejuízo.

- Ataques à camada da aplicação causaram a maior parte dos danos. Dois terços dos participantes da pesquisa passaram por ataques à aplicação. Um terço prevê vulnerabilidades de aplicação como uma grande preocupação em 2019, especialmente em ambientes na nuvem. Mais de metade fez mudanças e atualizou aplicações mensalmente, enquanto o restante fez atualizações com mais frequência, aumentando a necessidade por segurança automatizada.
- Os ataques virtuais que resultaram em uma interrupção completa dos serviços cresceram em 15% e uma em cada seis organizações relataram terem sofrido um ataque de 1 Tbps.
- Os hackers encontraram novas táticas para derrubar redes e data centers: Inundações de HTTPS cresceram em 20%, ataques de DNS e Burst attacks cresceram em 15% e ataques por bots, em 10%.
- Um terço das empresas relataram terem sofrido ataques para os quais não puderam identificar o motivo.

Preparação para o que vem pela frente

As organizações indicam que entendem a seriedade do cenário de ameaças que está mudando e estão tomando medidas para proteger seus ativos digitais, mas a severidade das ameaças à segurança é bem pesada.

- Quase metade se sentiu mal preparada para se defender contra todos os tipos de ciberataques, apesar de ter soluções de segurança instaladas.
- 86% dos negócios exploraram soluções de aprendizagem automática e inteligência artificial (IA) nos últimos 12 meses. Quase metade disse que os tempos de resposta mais rápidos aos ciberataques foram a motivação. A Radware viu um crescimento de 44% naqueles que conduzem seus negócios com blockchains.
- As empresas continuaram a diversificar as operações de rede entre vários provedores na nuvem. Duas em cada cinco organizações usam soluções de segurança virtual híbridas que combinam proteção no local e baseada em nuvem.
- 49% das organizações na EMEA disseram que não estavam bem preparadas para o GDPR.

A única opção é o sucesso

O custo dos ciberataques é simplesmente grande demais para não ter êxito em mitigar toda ameaça, o tempo todo. A confiança do cliente é destruída em alguns momentos, e o impacto é significativo na reputação da marca e nos custos para recuperar os negócios. O GDPR e outros regulamentos governamentais têm a capacidade de falir negócios que não estão em conformidade.

É crucial que as organizações incorporem a segurança virtual em seus planos de crescimento a longo prazo. Proteger os ativos virtuais não pode mais ser delegado apenas ao departamento de TI. Em vez disso, o planejamento de segurança precisa ser infundido nas novas ofertas de produtos e serviços, na segurança, nos planos de desenvolvimento e nas novas iniciativas de negócios. A equipe de CEOs e executivos precisa tomar a dianteira no caminho para estabelecer o tom e investir na segurança da experiência de seus clientes.

Perspectiva da diretoria

Os CEOs são os novos encarregados da confiança

A segurança virtual está se tornando um tópico muito pessoal para os executivos encarregados de liderar as empresas no nível mais alto. Para criar e manter relacionamentos sólidos com os clientes, os CEOs devem assumir o papel adicional de "diretor encarregado da confiança". Quando os anos de curadoria da estratégia da marca podem ser destruídos em um ciberataque, atribuir a estratégia de segurança ao diretor de segurança de informações (CISO) não é mais o suficiente. Há muita coisa em risco.

Considere os destinos dos CEOs nas empresas com brechas de grande importância como a Equifax, Yahoo, Moller-Maersk e Anthem Healthcare. Todo o trabalho que as organizações tiveram para construir o valor de suas marcas evaporou no momento em que os clientes perderam a confiança como resultado dos ataques. Não demorou muito e os CEOs da maioria dessas empresas foram "em busca de outros interesses".

Para garantir que a segurança virtual seja parte integral dos modelos de negócios das empresas, os CEOs precisam verificar os esforços e financiar medidas protetivas. Os CEOs que delegam a estratégia de segurança sem supervisioná-la estão arriscando seus cargos.

Faça o download do relatório gratuito

Relatório Global de Segurança de Rede e Seguraná de Aplicações